

United States District Court, Northern District of Illinois

| | | | |
|---|---|---|--------------|
| Name of Assigned Judge or Magistrate Judge | Robert M. Dow, Jr. | Sitting Judge if Other than Assigned Judge | Maria Valdez |
| CASE NUMBER | 08 C 3939 | DATE | 9/4/2008 |
| CASE TITLE | Mintel International Group, Ltd vs. Meesham Neergheen | | |

DOCKET ENTRY TEXT

This matter is before the Court on Plaintiff's Motion to Compel Datamonitor's Compliance with Subpoena [Doc. No. 53]. The matter is fully briefed and a hearing on the motion was held on September 3, 2008. The Plaintiff's Motion to Compel Datamonitor's Compliance with Subpoena [Doc. No. 53] is **DENIED** without prejudice. The Plaintiff and Datamonitor are directed to meet and confer before filing any additional motions on access to Datamonitor's computers.

■ [For further details see text below.]

Docketing to mail notices.
*Copy to judge/magistrate judge.

STATEMENT

In this case, Plaintiff alleges violations of Defendant's employment contract and non-compete agreement as well as alleged violations of the Illinois Trade Secret Act and the Computer Fraud and Abuse Act. The motion presently before the court seeks to compel third-party Datamonitor (Defendant's current employer) to provide Plaintiff access to Defendant's work computer and email and to compel production of Plaintiff's immigration (work authorization) documents.

On July 21, 2008 Plaintiff served third-party Datamonitor with a subpoena duces tecum requesting, in relevant part:

6. Produce all documents, including correspondence, that refer to Meesham Neergheen's status as an immigrant in the United States of America.
7. Produce all documents, including correspondence, that refer to, relate to or constitute the means of Meesham Neergheen's entry into the United States of America.
8. Permit forensic imaging and/or copying of all of Datamonitor's desktop and/or Laptop computers used at any time by Meesham Neergheen.
9. Permit the forensic imaging and/or copying of Meesham Neergheen's electronic mail account at Datamonitor.

(Pltf's Mot. Compel, Ex. 3)

On August 4, 2005, third-party Datamonitor lodged objections to the subpoena *duces tecum* based on relevancy, broadness, burden and privilege. (Datamonitor's Reply, Ex. E). On August 28, 2008 Plaintiff filed this Motion to Compel.

STATEMENT

Rule 26(b)(1) of the Federal Rules of Civil Procedure prescribes the scope of matters upon which a party may seek discovery. “Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party. . . . Relevant information need not be admissible at trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.” Fed.R.Civ.P. 26(b)(1). If the discovery is relevant, the party objecting to the discovery request bears the burden of showing why that request is improper. *Rubing v. Islamic Republic of Iran*, 349 F. Supp. 2d 1108, 1111 (N.D. Ill. 2004). Rule 26© authorizes courts, for good cause, to “make any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including . . . that certain matters not be inquired into, or that the scope of the disclosure or discovery be limited to certain matters . . .” Fed.R.Civ.P. 26©. The trial court will use its broad discretion in resolving matters relating to discovery. *Patterson v. Avery Dennison Corp.*, 281 F.3d 676, 681 (7th Cir. 2002).

In exercising its discretion under Rule 45, this Court must engage in a balancing process that includes consideration of the likelihood that compliance will result in production of the information, whether the discovery is cumulative, whether the information sought is readily obtainable from another less burdensome source, and whether the burden of the proposed discovery outweighs its likely benefit. *See Northwestern Memorial Hospital v. Ashcroft*, 362 F.3d 923, 927 (7th Cir.2004); *Watts v. S.E.C.*, 482 F.3d 501, 509 (D.C.Cir.2007). Further, when discovery is sought from a third-party the normal standard of *possible* relevance may not be enough and the third-party can be entitled to somewhat greater protection. *See Builders Ass'n of Greater Chicago v. City of Chicago*, 2001 WL 664453 at *7 n. 4 (N.D.Ill. June 12, 2001). Such protection includes weighing the need for the material subpoenaed against the interests that enforced production would compromise or injure the third-party involved in its production. *Northwestern Hospital*, 362 F.3d at 928-29.

Access to Datamonitor's Electronic Data

Plaintiff seeks access to Datamonitor's computer(s), including email accounts, used by Defendant in his employment. Defendant acknowledges that before he left Mintel he emailed to his personal e-mail account Mintel documents. He has testified that he did not share any of the Mintel documents with Datamonitor and did not transfer the documents in electronic format to any other device or computer. (Datamonitor Reply, Ex. C at 162-170). Plaintiff wishes to check the veracity of this and seeks access to Datamonitor's computer and email used by Defendant.

In filing this motion, the only issue of relevancy raised by the Plaintiff concerned spoliation. Eleven (11) of the twelve (12) and one half pages of the Motion before this Court discuss spoliation and no other relevancy theory. Nonetheless, in its Reply, Plaintiff raises for the first time the argument that the requested information is also relevant to the merits of the case. That is, Plaintiff argues that not only would the requested information be relevant to show spoliation of evidence, but it could be relevant to a claim or defense in this case. Traditionally, where a movant “failed to discuss the facts relevant to their claim,” such “[p]erfunctory or undeveloped arguments are waived.” *Estate of Moreland v. Dieter*, 395 F.3d 747, 759 (7th Cir. 2005) (citing *Colburn v. Trs. of Ind. Univ.*, 973 F.2d 581, 593 (7th Cir. 1992); *Hunter v. Allis-Chalmers Corp.*, 797 F.2d 1417 (7th Cir. 1986). Similarly, arguments raised for the first time in a reply brief are generally treated as waived. *See Walker v. Wallace Auto Sales, Inc.*, 155 F.3d 927, 930 (7th Cir.1998).

Therefore, this Court will evaluate the entitlement to discovery based on the potential relevancy of the information sought to the issue raised in their moving papers – the spoliation argument. To determine possible relevancy under a spoliation theory this court need not look any further than the district court's order of July 16, an order drafted by the Plaintiff. Plaintiff secured an order from the district court requiring

STATEMENT

Defendant to produce a forensic copy of all personal laptop and desktop computers. The order also prohibited Defendant “from deleting any files from his personal desktop and/or laptop computer relating to or taken from Mintel.” See July 16, 2008 Order [Doc. No. 14].

Plaintiff points out the Defendant did not hand over his computer until July 18. Plaintiff also points out that the complaint was filed on July 11, 2008 and Defendant was under a duty to preserve based on the filing of the complaint. Under Plaintiff’s spoliation theory, the relevant time frame is this one week period. After receipt of the Defendant’s computer, Plaintiff undertook a forensic evaluation of the computer. The forensic evaluation of the computer provides the sole support for the motion to compel access to Datamonitor’s computer. The Court has reviewed the affidavit submitted by Mr. Jones. According to the forensic expert Jones [Pltf’s Mot., Ex. 1], the following conclusions were drawn from the forensic analysis:

1. Over 3,900 new files were created on or after July 13, 2008;
2. About 98 files were reported as deleted and include Windows system restore point files and Skype communication tool files;
3. The running of the McAfee virus automatic system tool could have altered the time/date metadata for file entries;
4. A review of the internet search history disclosed a number of search terms used on the Microsoft website that include “how%20do%i%access” “deleted”;
5. Some internet history data was presumed missing;
6. A portion of the Windows registry was deleted;
7. The hard drive was defragmented using a Windows defragmentation utility.

Based on these conclusions, the Plaintiff believes that accessing the Datamonitor computer would lead to relevant information that may show that Mintel documents were downloaded onto Datamonitor computers. The first step is to determine whether accessing the Datamonitor computer would lead to relevant information. Plaintiff is asking the district court to sanction Plaintiff based on a spoliation theory. To determine relevancy of discovery on this spoliation theory the Court must determine the relevant standard for spoliation.

Generally, once a party reasonably anticipates litigation, it must put in place a litigation hold to ensure the preservation of relevant documents. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y.2003). Based on the district court’s order of July 16 (as requested by the Plaintiff) the “relevant” documents that must be preserved are files “relating to or taken from Mintel.” Plaintiff argued at the hearing that the relevant documents to be preserved prior to the entry of the Court’s order are broader than that requested from the Court on July 16. This makes no sense. The Plaintiff’s defined for the district court what they considered to be “relevant.” What is “relevant” on July 11 should not be any different from what is relevant on July 16.

Based on this standard of relevancy, the Court then has to determine whether the information sought would reasonably lead to the admission of relevant spoliation evidence taking into consideration the factors listed above. Plaintiff relies heavily on the Jones Affidavit to demonstrate that deletion of files may have occurred. However, the Jones Affidavit is broad and general in nature. Jones focuses on a standard of spoliation that is not present in this case. According to Jones, because Defendant turned on the computer that could result in spoliation. But, the standard for spoliation under the district court’s order is whether Defendant deleting files “relating to or taken from Mintel.” Most of the Jones affidavit describes activity that is not, on its face, prohibited under the Court Order. Merely turning on the computer, accessing the internet or deleting files not related to Mintel is not covered by the Court’s Order.

STATEMENT

As to deleted files, the Jones affidavit does not describe whether there were any deleted files that were unrecoverable or even whether any of the deleted files were ultimately overwritten so as to become unrecoverable. To the contrary, the Reisman affidavit submitted by Datamonitor (Datamonitor Opp., Ex. F) counters the Jones affidavit point for point and sets forth examples as to how the deletion of files identified by Jones is not really deleted. For example, according to Reisman running a defragmentation utility does not necessarily result in unrecoverable files. (Ex. F, at p. 10).

The justification Plaintiff has advanced for the computer access is not enough. This is so especially in light of the fact that the requested information would come from a third-party competitor. Because they have not established that accessing Datamonitor's computer would lead to relevant evidence of spoliation the motion for access is denied without prejudice. Plaintiff may reassert relevancy to this information as it pertains to the merits of the case at a later time.

Immigration Documents

In addition, Plaintiff Mintel has requested documents related to Defendant's immigration status from third-party Datamonitor. Plaintiff originally propounded document requests to the Defendant which included requesting the work authorization documents at issue in this motion. On July 24, 2008, Defendant objected to this document production request on relevancy and privilege grounds. (Pltf's Reply, Ex. 2 at 13). Plaintiff chose not to compel production from Plaintiff. Instead, Defendant sought the documents from Datamonitor. Third-party Datamonitor objected to the request on relevancy grounds.

Plaintiff Mintel claims that discovery related to Defendant's immigration status is relevant to ascertain Neergheen's start date with Datamonitor, and is not an undue burden. Datamonitor claims that any discovery related to Defendant's immigration status is irrelevant to the claims in the lawsuit.

This is an action for a violation of terms of Defendant's employment contract and non-compete agreement as well as alleged violations of the Illinois Trade Secret Act and the Computer Fraud and Abuse Act. The Court finds that inquiries into immigration status are simply not relevant to the claims and defenses in this case. Whether the Defendant was authorized to work in the United States has no bearing on whether he violated the non-compete agreement he entered into or the Illinois Trade Secret Act and Computer Fraud and Abuse Act.

Courts have recognized the potentially damaging effects of allowing inquiries into a litigant's immigration status. *See EEOC v. Bice of Chicago*, 229 F.R.D. 581, 582 (N.D. Ill.2005) ("questions about immigration status are oppressive"); *see also EEOC v. First Wireless Group, Inc.*, 225 F.R.D. 404 (E.D.N.Y.2004) (disclosure of immigration status could cause embarrassment, potential criminal charges, or deportation if status was discovered to be illegal). Here, Defendant's immigration status and work authorization are collateral issues. Whether Defendant was authorized to work in the United States simply has no bearing on whether he violated the terms of his employment contract and non-compete agreement or the Illinois Trade Secret Act and Computer Fraud and Abuse Act.

Lastly, Plaintiff also asserts that the documents requested would allow them to test the truthfulness of Neergheen's testimony and representations made by Neergheen's counsel as to his start date. While credibility is always at issue, that "does not warrant unlimited inquiry into the subject of immigration status . . ." *Avila-Blum v. Casa de Cambio Delgado, Inc.*, 236 F.R.D. 190, 192 (S.D.N.Y.2006).